IN THE SPECIFICATION

Please amend page 8, second full paragraph commencing at line 11, as follows:

The following patents, ~~expressly incorporated herein by reference,~~ provide enhanced security features for use with finished paper and for non-currency and non-security papers. EP-A2-0203499 discloses a method of applying a pseudo watermark to paper. This method comprises the preparation of a paper containing thermally sensitive material, the presence of which renders the translucency of the paper variable by temperature change. When heat is subsequently applied to a part of the surface of the paper, a region of the paper becomes semi-translucent. U.S. Pat. No. 2,021,141 (Boyer, November 1935), expressly incorporated herein by reference, discloses a method of applying pseudo watermarks to paper, by applying a resinous composition to finished paper which permeates the paper and causes it to become more transparent, or translucent, than the surrounding area. GB-A-1489084 describes a method of producing a simulated watermark in a sheet of paper. The sheet is impregnated in the desired watermark pattern with a transparentising composition which, when submitted to ultra violet radiation, polymerizes to form a simulated watermark. U.S. Pat. No. 5,118,526 (Allen, et al., June 2, 1992), expressly incorporated herein by reference, describes a method of producing simulated watermarks by applying heat, in the desired watermark pattern, onto a thin solid matrix of waxy material placed in contact with a sheet of paper. This results in an impression of a durable translucent watermark. U.S. Pat. No. 4,513,056 (Vernois, et al., April 23, 1985), expressly incorporated herein by reference, relates to a process for rendering paper either wholly or partially transparent by impregnation in a special bath of a transparentization resin and subsequent heat cross-linking of the resin. EP-A1-0388090 describes a method of combining a see-through or print-through feature with a region of paper which has a substantially uniform transparency which is more transparent than the majority of the remainder of the sheet. JP 61-41397 discloses a method for making paper transparent and a method for its manufacture for see-through window envelopes. The method utilises the effect of causing ink cross-linked by ultra-violet rays to permeate paper thus causing that part of the paper to become transparent.

IN THE SPECIFICATION

Please amend page 28, first new paragraph, commencing at line 23, as follows:

It is known to provide a number of different types messages for cryptographic authentication. A so-called public key/private key encryption protocol, such as available from RSA, Redwood Calif., may be used to label the workpiece with a "digital signature". See, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems" by R. L. Rivest, A. Shamir and L. Adelmann, Communications of ACM 21(2):120-126 (February 1978)~~, expressly incorporated herein by reference~~. In this case, an encoding party codes the data using an appropriate algorithm, with a so-called private key. To decode the message, one must be in possession of a second code, called a public key because it may be distributed to the public and is associated with the encoding party. Upon use of this public key, the encrypted message is deciphered, and the identity of the encoding party verified. In this scheme, the encoding party need not be informed of the verification procedure. Known variations on this scheme allow private communications between parties or escrowed keys to ensure security of the data except under exceptional authentication procedures. See also, W. Diffie and M. E. Hellman, "New directions in cryptography", IEEE Trans. Information Theory, Vol. IT-22, pp. 644-654, November 1976; R. C. Merkle and M. E. Hellman, "Hiding information and signatures in trapdoor knapsacks", IEEE Trans. Information Theory, Vol. IT-24, pp. 525-530, September 1978; Fiat and Shamir, "How to prove yourself: practical solutions to identification and signature problems", Proc. Crypto 86, pp. 186-194 (August 1986); "DSS: specifications of a digital signature algorithm", National Institute of Standards and Technology, Draft, August 1991; and H. Fell and W. Diffie, "Analysis of a public key approach based on polynomial substitution", Proc. Crypto. (1985), pp. 340-349~~, expressly incorporated herein by reference~~. Another encoding scheme uses a DES-type encryption system, which does not allow decoding of the message by the public, but only by authorized persons in possession of the codes. This therefore requires involvement of the encoding party, who decodes the message and assists in authentication.

SPECIFICATION

Please amend page 30, second and third complete paragraphs commencing on line 15, as follows:

Methods that hide validation information within the data being authenticated offer an alternative means to validate digital data. Digital watermarks can be added to data by methods falling generally into the field of steganography. Steganographic methods are reviewed by W. Bender, D. Gruhl, and N. Morimoto in "Techniques for Data Hiding," Proc. SPIE, Storage and Retrieval for Image and Video Databases III, 9-10 Feb., 1995, San Jose, Calif. ~~This reference also is incorporated herein by reference.~~

One method of impressing a digital watermark is given by G. Caronni, in "Assuring Ownership Rights for Digital Images," Proc. Reliable IT Systems, VIS '95, 1995, edited by H. H. Bruggemann and W. Gerhardt-Hackl (Vieweg Publ. Co.: Germany). Another method is given by I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon in "Secure Spread Spectrum Watermarking for Multimedia," NEC Research Inst. Tech. Report 95-10, 1995. ~~These references also are incorporated herein by reference.~~

SPECIFICATION

Please amend page 33, first complete paragraph, commencing at line 13, as follows:

A digital signature standard (DSS) has been developed that supplies a shorter digital signature than the RSA standard, and that includes the digital signature algorithm (DSA) of U.S. Pat. No. 5,231,668 (Kravitz, July 27, 1993). This development ensued proceeding from the identification and signature of the U.S. Pat. No. 4,995,081 (Leighton, et al., February 19, 1991), expressly incorporated herein by reference, and proceeding from the key exchange according to U.S. Pat. No. 4,200,770 (Hellman, et al., April 29, 1980), expressly incorporated herein by reference, or from the El Gamal method (El Gamal, Taher, "A Public Key Cryptosystem and a Singular Scheme Based on Discrete Logarithms", 1 III Transactions and Information Theory, vol. IT-31, No. 4, Jul. 1985)~~, all of which are expressly incorporated herein by reference~~.

SPECIFICATION

Please amend page 33, fourth paragraph, commencing on line 27, as follows

Typical encryption and document encoding schemes that may be incorporated, in whole or in part, in the system and method according to the invention, to produce secure certificates and/or markings, are disclosed in U.S. Pat. Nos. 5,422,954 (Berson, June 6, 1995); 5,337,362 (Gormish, et al. August 9, 1994); 5,166,978 (Quisquater, November 24, 1992); 5,113,445(Wang, May 12, 1992); 4,893,338 (Pastor, January 9, 1990); 4,879,747(Leighton, et al., November 7, 1989); 4,868,877 (Fischer, September 19, 1989); 4,853,961(Pastor, August 1, 1989); and 4,812,965 (Taylor, March 14, 1989), expressly incorporated herein by reference. See also, W. Diffie and M. E. Hellman, "New directions in cryptography", IEEE Trans. Information Theory, Vol. IT-22, pp. 644-654, November 1976; R. C. Merkle and M. E. Hellman, "Hiding information and signatures in trapdoor knapsacks", IEEE Trans. Information Theory, Vol. IT-24, pp. 525-530, September 1978; Fiat and Shamir, "How to prove yourself: practical solutions to identification and signature problems", Proc. Crypto 86, pp. 186-194 (August 1986); "DSS: specifications of a digital signature algorithm", National Institute of Standards and Technology, Draft, August 1991; and H. Fell and W. Diffie, "Analysis of a public key approach based on polynomial substitution", Proc. Crypto. (1985), pp. 340-349~~, expressly incorporated herein by reference~~.